Scientific Research Journal of Engineering and Computer Sciences
ISSN (Print) : 2788-9394 & ISSN (Online) : 2788-9408
Language : English
DOI Prefix: 10.47310/srjecs
Website : https://iarconsortium.org/srjecs/

Case Report

Social Engineering and Its Role in Maintaining Information Security and Privacy

Article History
Received: 5 Oct, 2024
Revised: 20 Oct, 2024
Accepted: 20 Nov, 2024
Published: 23 Dec, 2024

Author Details
Hussein Falah Aboalhab[1] and Dr. Mohamed Farhat[2]

Authors Affiliations
[1]Assistant Teacher, Islamic University / Faculty of Law Master of Public International Law, Iraq
[2]Supervision Professor, Islamic University / Faculty of Law Master of Public International Law

Corresponding Author*
Hussein Falah Aboalhab

DOI: 10.47310/srjecs.2024.v04.i02.010

How to Cite the Article:
Hussein Falah Aboalhab & Mohamed Farhat. 2024 ; Social Engineering and Its Role in Maintaining Information Security And Privacy, *IAR Journal Medical Case Reports*, V5 I2; Pp: 1.-10.

Abstract: In this study, we seek to achieve a main goal, which is to identify social engineering and its role in maintaining information security and privacy, introducing the risks of social engineering, the spread of social engineering, and identifying the role of information security in the face of social engineering and how the personal characteristics of individuals affect their vulnerability to exploitation, and this study is considered one of the descriptive studies that relied on the content analysis methodology, by reviewing previous studies, interviews and research. The study concluded with a number of recommendations, including that social engineering should be controlled or at least limited when it comes to information security, as many people focus on technical security as technical solutions such as firewalls, authentication rules, encryption, access restrictions and permissions are necessary for information security in the organization because they can prevent attacks.

Keywords: Social Engineering, Cybercrime, Information Security, Privacy, Human Behavior.

INTRODUCTION

أهمية موضوع البحث: تظهر أهمية الدراسة من خلال قلة الأبحاث المتعلقة بموضوعها وفق علم الباحث، وتساهم هذه الدراسة في إثراء المجال المعرفي حول ظاهرة الهندسة الاجتماعية في العالم الرقمي وكيفية الوقاية من مخاطرها بالإضافة إلى انتشار وسائل الاتصال وبالأخص برامج التواصل الاجتماعي وأن هذه البرامج أصبحت شكل من أشكال الحياة في وقتنا الحاضر، فإن هذه الدراسة تسعى للتعرف على الهندسة الاجتماعية ودورها في الحفاظ على أمن المعلومات والخصوصية.

إشكالية البحث: انطلقت مشكلة الدراسة من خلال تساؤلاً رئيساً هو التعرف على الهندسة الاجتماعية ودورها في الحفاظ على أمن المعلومات والخصوصية وينبثق عن هذا التساؤل الرئيسي عدة تساؤلات فرعية وهي على النحو التالي:

- هل تأثر السمات الشخصية للأفراد في قابليتهم للاستغلال؟
- ماهي هجمات الهندسة الاجتماعية القائمة على التكنولوجيا؟
- ما الاستراتيجيات المستخدمة في الهندسة الاجتماعية من خلال الدراسات والمقابلات؟
- ماهي تطبيقات الهندسة الاجتماعية في مجال أمن المعلومات؟
- ما هو أشكال التعاون بين الهندسة الاجتماعية والتقنيات الأمنية؟

الهدف من البحث: انطلاقاً من مشكلة الدراسة، نسعى لتحقيق هدفاً رئيساً هو التعرف على الهندسة الاجتماعية ودورها في الحفاظ على أمن المعلومات والخصوصية وينبثق عن هذا الهدف الرئيسي عدة أهداف فرعية وهي:

- التعرف على تأثير السمات الشخصية للأفراد في قابليتهم للاستغلال.
- التعرف على هجمات الهندسة الاجتماعية القائمة على التكنولوجيا.
- تحليل الاستراتيجيات المستخدمة في الهندسة الاجتماعية من خلال الدراسات والمقابلات.
- التعرف على تطبيق الهندسة الاجتماعية في مجال أمن المعلومات.
- التعرف على التعاون بين الهندسة الاجتماعية والتقنيات الأمنية.

المقدمة:

تمثل الهندسة الاجتماعية أحد أقوى أشكال الجرائم السيبرانية وأكثرها استمراراً، وثمة سبب يقف وراء الانتشار الواسع للهندسة الاجتماعية في أوساط مجرمي الإنترنت، إذ إن اختراق بيانات الأشخاص أسهل بكثير من اختراق البرامج الكمبيوترية. والهندسة الاجتماعية عبارة عن مجموعة من الحيل والتقنيات المستخدمة لخداع الناس.

مع التقدم المتنامي في التكنولوجيا، تتزايد التهديدات والمخاطر الأمنية. إذ أصبح مجرمو الإنترنت متطورين بشكل متزايد في الطرق التي يستغلون بها التكنولوجيا، مما يجعل من الصعب القضاء على المخاطر. وعليه يمكن أن تكون الهجمات السيبرانية على البنية التحتية التكنولوجية في شكل برامج ضارة وفيروسات، أو على الأفراد البشريين، في شكل الهندسة الاجتماعية أو البلطجة السيبرانية [1]

يسعى مجرمو الإنترنت الذين يستخدمون الهندسة الاجتماعية إلى خداع ضحاياهم حتى يقدموا طوعاً معلوماتهم الشخصية[2] إذ تم إنشاء الهندسة الاجتماعية على أساس مصطلحات نفسية وأمنية [3] من قبل مختلف المنظمات والخبراء، حيث يتم الاستفادة من سذاجة الأشخاص الضعفاء عن طريق التأثير، في جوانب مختلفة مثل الإقناع والتلاعب للحصول على معلومات حيوية[4] من خلال معرفة المعلومات الشخصية أو ما شابه ذلك الشخص، يصبح الشخص بلا دفاع حتى يتمكن المهاجمون من معرفة بنية كلمات المرور الخاصة بهم. يستخدم مستخدمو الشبكات الاجتماعية، مثل مستخدمي Facebook و Instagram و Youtube وTwitter والمدونات وغيرهم من مستخدمي وسائل التواصل الاجتماعي الحالية، الشبكات الاجتماعية كنافذة عالمية يعرضون فيها جوانب متعددة من حياتهم اليومية[5]، لأغراض مختلفة. وبعضها تجاري واضح في الوقت الحاضر، يتم تقديم الجرائم الإلكترونية من قبل المتسللين عبر شبكات التواصل الاجتماعي، لأن لديهم القدرة على تحديد طرق إعادة توجيه الرسائل غير المرغوب فيها لأغراض إعلانية بطريقة غير قانونية[6].

المطلب الأول: مفهوم الهندسة الاجتماعية واسسها

الفرع الأول: تعريف الهندسة الاجتماعية

عرفها صاحب كتاب الهندسة الاجتماعية "فن اختراق البشر" بأنها: فعل التلاعب بالشخص لاتخاذ إجراء معين قد يكون أو لا يكون في مصلحته، ويمكن أن يشمل الحصول على المعلومات، حق الوصول للهدف لاتخاذ اجراءات معينه[7].

وعرفت أيضاً شكل شائع من أشكال الجريمة الإلكترونية[8]. يشار إلى فعل الحصول على الوصول غير المصرح به إلى نظام أو معلومات حساسة، مثل كلمات المرور، باستخدام الثقة وبناء العلاقات مع الآخرين الذين يمكنهم الوصول إلى هذه المعلومات باسم الهندسة الاجتماعية. يحاول ما يقرب من 3٪ فقط من البرامج الضارة الاستفادة من عيب تكنولوجي. تتضمن نسبة 97٪ الأخرى استهداف المستخدمين من خلال الهندسة الاجتماعية.

ولقد ورد تعريف الهندسة الاجتماعية في 27 قاموس متخصص في قاعدة بيانات[9] (Onelook) ، ونجد بأن مفهوم الهندسة الاجتماعية يختلف وفقاً للتخصصات العلمية وطبيعة السياق المستخدم، فمصطلح الهندسة الاجتماعية في العلوم السياسية مرتبط بقضايا التأثير على مواقف الأفراد والجماعات أو استخدام مختلف الأساليب للتأثير على مواقف معينة وسلوكيات اجتماعية على نطاق واسع، كما تعرف أيضًا بأنها استخدام التخطيط المركزي في محاولة لإدارة التغيير الاجتماعي .(Oxford Dictionaries) أما عن مفهوم الهندسة الاجتماعية عند الحديث عن الأمن أو أمن المعلومات، فتتمثل في خداع الناس أو التلاعب بهم للإفصاح عن معلومات تتمتع بالسرية أو الخصوصية. ففي سياق أمن المعلومات يشير المصطلح كما ورد في قاموس (Dictionaries Oxford) إلى استخدام أساليب الخداع للتلاعب بالأفراد بهدف الحصول على معلومات سرية أو شخصية يمكن استخدامها لأغراض احتيالية ويربط قاموس (of Computing) مصطلح الهندسة الاجتماعية بعمليات الاحتيال والخداع للحصول على معلومات سرية باستخدام مجموعة من الأساليب وتقنيات مختلفة. وعند الحديث عن مفهوم الهندسة الاجتماعية كما ورد في النتاج الفكري، فيعرفها Granger (2001) بأنها فن التلاعب بعقول الأفراد لكسب الثقة وتحقيق الغاية، وبالتالي فهي وسيلة ذكية للحصول على الرقم السري لمستخدم دون الحاجة لخرق النظام تقنيًا. ومهما اختلفت مفاهيم الهندسة الاجتماعية، فالمغزى المراد تحقيقه هو الحصول على بيانات تتمتع بطابع عالي من الخصوصية والسرية، ويمكن النظر أيضًا للهندسة الاجتماعية من منظور معلوماتي، فيرى المتخصصون في مجال المعلومات بأن استخدام المصطلح مرتبط بالبيانات والمعلومات، فالوصول إلى البيانات ومعالجتها يكشف عن معلومات يستفاد منها لتحقيق غايات أخرى.

يعرف Engebretson الهندسة الاجتماعية بأنها إحدى أبسط الطرق لجمع المعلومات حول هدف ما من خلال عملية استغلال الضعف البشري الموروث في كل منظمة[10] في جوهرها، تشير الهندسة الاجتماعية إلى تصميم وتطبيق تقنيات خادعة للتلاعب عمداً بالأهداف البشرية. وفي سياق الأمن السيبراني يتم استخدامه في المقام الأول لحث الضحايا على الكشف عن البيانات السرية، أو القيام بأعمال تنتهك البروتوكولات الأمنية، أو إصابة الأنظمة دون

([1])Sarathchandra, D. Haltinner, K. and Lichtenberg, N. "College students' cybersecurity risk perceptions, awareness, and practices," in Proc. Cybersecurity 3rd Symp. (CYBERSEC '16), Coeur d'Alene, ID, 2016, pp. 68-73.

(2) Grande,C. E. L., and Guadrón, R. S., "Social Engineering: The Silent Attack," no. Concapan Xxxv, 2015.

(3) Centre, C. S. and Jones, A., "Information Security and Digital Forensics in the world of Cyber Physical Systems," pp. 10-14, 2016.

(4) Ghafir, I. Prenosil, V, Alhejailan, A. and Hammoudeh, M. "Social Engineering Attack Strategies and Defence Approaches," 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, pp. 145-149, 2016.

(5) Rachsuda, J. "User preferences profiling based on user behaviors on facebook page categories," pp. 248-253, 2017.

(1) Bhise, K., "A Method For Recognize Malignant Facebook Application," pp. 41-44, 2016.

(2) Christopher,h., Social Engineering: The Art of Human Hacking, (2017)، WILEY Publishing.

(3) Frumento, E. Estimates of the Number of Social Engineering Based Cyber-Attacks into Private or Government Organizations. Dogana Project. (2018)

([9]) الكندي، سالم بن سعيد بن علي، و حليمه سليمان البلوشي. "الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة." مجلة الآداب والعلوم الاجتماعية مج11, ع2 (2020): 71 - 84.

(1) Nabie Y Conteh, Paul J Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks", International Journal of Advanced Computer Research, Vol.6 pp.23-31, 2016.

قصد، أو إطلاق معلومات سرية[11] أساس هجوم الهندسة الاجتماعية هو تجنب أنظمة الأمن السيبراني من خلال الخداع، واستغلال الحلقة الأضعف، أي الأشخاص المعنيين[12].

الفرع الثاني: أسس الهندسة الاجتماعية [13]

في الهجوم السيبراني، يكون المهاجم والضحية (الهدف) كيانين على الطرفين. بالنسبة للهندسة الاجتماعية، فإن المهاجم (المعروف أيضًا باسم المهندس الاجتماعي) هو الطرف الذي يقوم بهجوم الهندسة الاجتماعية، الضحية هو الطرف الذي يتعرض لهجوم الهندسة الاجتماعية ويتسبب في نتيجة الهجوم. بشكل عام يمكن وصف عملية هجوم الهندسة الاجتماعية على النحو التالي: 1) يقوم المهاجم بصياغة أساليب هجوم معينة لاستغلال نقاط الضعف البشرية للهدف وتحقيق أهداف هجومية معينة؛ 2) بمجرد استغلال نقاط الضعف البشرية، يتحول الهدف إلى ضحية ويؤدي إلى عواقب معينة للهجوم؛ 3) يقوم المهاجم بإرجاع النتائج إلى هدف الهجوم، ليقرر الإجراءات التالية:

هناك **ثلاث** وجهات نظر أساسية لفهم كيفية تأثير هجمات الهندسة الاجتماعية: -

أ. من وجهة نظر المهاجم، أسلوب الهجوم هو الطريقة أو الطريقة أو الوسيلة لتنفيذ الهجوم؛ إنها أيضاً القوة الدافعة التي تتسبب بشكل مباشر في هجوم الهندسة الاجتماعية وتؤثر بشكل كبير على إمكانية نجاح الهجوم. بعد كل شيء، أساليب الهجوم المتقدمة والمبتكرة عادة ما تمتلك نسبة نجاح أكبر للحصول على أهداف الهجوم.

ب.

ت. من وجهة نظر الضحية، فإن نقاط الضعف البشرية المستغلة هي السبب الجذري لعواقب الهجوم. وتتمثل إحدى نقاط التعارض بين هجمات الهندسة الاجتماعية والدفاعات في أن نقاط الضعف البشرية هي تلك التي يريد المهاجمون استغلالها وتلك التي يريد الضحايا القضاء عليها أو التخفيف من حدتها. يمكن استغلال أنواع أخرى من نقاط الضعف (مثل نقاط الضعف البرمجية) إلى جانب نقاط الضعف البشرية، ولكنها ليست أساسية في هجمات الهندسة الاجتماعية.

ث.

ج. من منظور المبدأ والشرح، تشرح آليات التأثير كيف تؤثر أساليب الهجوم على نقاط الضعف البشرية. تصف آليات التأثير [R1] كيف تستغل أساليب الهجوم قدرات الضعف البشري، وتشرح [R2] لماذا تؤدي نقاط الضعف البشرية إلى عواقب الهجوم وكذلك المقابلة)[R3] كيف تحقق أساليب الهجوم أهداف الهجوم. وبعبارة أخرى، يمكن تعريف آليات التأثير على أنها العلاقة الهيكلية التي تتوافق فيها عواقب الهجوم المحدد ولماذا أو كيف مع نقاط ضعف بشرية محددة، في سيناريوهات هجوم محددة. وبالتالي، يمكن أن تكون آلية التأثير والضعف البشري وطريقة الهجوم بمثابة ثلاثة كيانات أساسية للحصول على نظرة ثاقبة حول كيفية عمل هجمات الهندسة الاجتماعية وتأثيرها.

ح.

الفرع الثالث: علم النفس والسلوك البشري

الطبيعة البشرية هي مجموعة من الخصائص النفسية على المستوى الكلي، تصف السمات النفسية الأساسية التي يشترك فيها الكائن البشري بأكمله بشكل طبيعي، فبعض الطبيعة البشرية عبارة عن ثغرات أمنية يمكن استغلالها في هجمات الهندسة الاجتماعية، الأشخاص الذين يولون اهتماماً وثيقاً لأنفسهم ورغباتهم سوف يضخمون التأثير المحيط بهم ويزيدون من قابلية الحث والإقناع والتلاعب في الهندسة الاجتماعية، إن الطلب الجامح على الإغراءات والخوف من استبعادهم من المكاسب المحتملة من شأنه أن يدفع الأشخاص ذوي الإرادة الضعيفة إلى اتخاذ قرارات ضعيفة أو سلوكيات خطيرة لذا فإن الطبيعة البشرية هي مثل حب الذات (النرجسية) والجشع والشهوة والتخمة تصبح نقاط ضعف يمكن استغلالها في بعض سيناريوهات هجمات الهندسة الاجتماعية [14]. من الطبيعي أن يتعاطف الناس مع الأفراد الذين يقعون في ورطة، ولذلك فإن التظاهر بأنك شخص يحتاج إلى المساعدة يثبت فعاليته مراراً وتكراراً في السماح للمهندسين الاجتماعيين بالوصول إلى أهدافهم[15].

تساهم السمات الشخصية للأفراد بشكل كبير في قابليتهم لاستغلال الهندسة الاجتماعية مثل التأثير والتلاعب والخداع [16]. ويتعامل المهندسون الاجتماعيون مع سمات الشخصية البشرية على أنها نقاط ضعف ويستخدمون اللغة كسلاح لخداع الضحايا وإقناعهم والتلاعب بهم في النهاية [17].

سمات الشخصية هي بنى نفسية أو مجموعات مميزة من الأنماط الاعتيادية للسلوك والتفكير والعاطفة التي تتطور من الوراثة البيولوجية، وتتأثر في المقام الأول بالعوامل البيئية. تختلف سمات الشخصية من فرد لآخر وتؤثر على سلوكه. إلى جانب ذلك، فإن سمات الشخصية مستقرة نسبياً بمرور الوقت ومواقف ثابتة في العديد من النظريات والنظم، يمكن تصنيف سمات الشخصية إلى أبعاد مختلفة ويمكن تصنيف السمات الفردية وفقاً لذلك. وينظم نموذج العوامل الخمسة للشخصية السمات الشخصية بشكل هرمي من حيث خمسة أبعاد أساسية: الانبساطية، والضمير، والاتفاقية، والانفتاح على التجربة، والعصابية أو الاستقرار النفسي أو العصابي[18]، وتتجلى سمات الشخصية في بُعد الانبساط بشكل أساسي في النشاط والدفء والمشاعر الإيجابية والحزم والبحث عن الإثارة والاجتماع،

(2) "Hacking the human operating system: The role of social engineering within cybersecurity", Technical report, Intel Security, 2015.
(3) Prashant, K, D., "Prashant's algorithm for password management system", International Journal of Engineering Science, pp.2424, 2016.
(1) Wang, Z. Sun, L. and Zhu, H. "Defining social engineering in cyber- security," IEEE Access, vol. 8, pp. 85094-85115, 2020, doi: 10.1109/ access.2020.2992807.
(1) Maseno, E. M. "Vishing attack detection model for mobile users," M.S. thesis, Comput. Inf. Manage., KCA Univ., Nairobi, Kenya, Nov. 2017. [Online]. Available: http://41.89.49.13:8080/xmlui/ handle/123456789/1276
(2) Maseno, E. M. "Vishing attack detection model for mobile users," M.S. thesis, Comput. Inf. Manage مرجع سابق
(1) J. Stewart and M. Dawson, "How the modification of personality traits leave one vulnerable to manipulation in social engineering," Int. J. Inf. Privacy, Secur. Integrity, vol. 3, no. 3, pp. 187-208, Jan. 2018.
(2) Tsinganos, N. Sakellariou, G. Fouliras, P. and Mavridis, I. "Towards an automated recognition system for chat-based social engineering attacks in enterprise environments," in Proc. 13th Int. Conf. Availability, Rel. Secure., New York, NY, USA, Aug. 2018, p. 53
(3) McCrae R. R. and John, O. P. "An introduction to the five-factor model and its applications," J. Personality, vol. 60, no. 2, pp. 175-215, Jun. 1992.

فالأفراد الذين يتمتعون بدرجة عالية من الانبساط هم أكثر نشاطاً وحماساً وحزماً وانفتاحاً وثرثرة. وبالتالي، فهم عرضة للهندسة الاجتماعية من خلال آليات التأثير مثل الإعجاب والمساعدة، والكشف عن الذات وبناء العلاقات، وإدارة الانطباع، والالتزام والاتساق، والمخاطرة من أجل الثقة والتوافق.

ويركز بعد الضمير على الكفاءة والنظام والإخلاص والانضباط الذاتي والسعي لتحقيق الإنجاز والمداولة، فالأشخاص في هذا النوع يعتبرون هم أكثر كفاءة وتنظيماً ومسؤولية وتخطيطاً وموثوقية ودقة وبالتالي، فهم عرضة للهندسة الاجتماعية من خلال آليات التأثير مثل الطريق المركزي للإقناع، والطاعة للسلطة، والتأثير المعلوماتي، ومعيار المسؤولية الاجتماعية، والواجب الأخلاقي، والالتزام والاتساق.

المطلب الثاني: أساليب الهندسة الاجتماعية

تمثل هجمات التصيد الاحتيالي تحديات أمنية خطيرة لأنها تعتمد على سلوك الأفراد أو المشتركين بدلاً من الاعتماد على ثغرة أمنية، مما يجعل التصيد الاحتيالي أحد أكثر تقنيات الهندسة الاجتماعية شيوعًا ونجاحاً[19] ويعد التصيد الاحتيالي أحد أكثر الأمثلة شيوعاً لتقنيات الهندسة الاجتماعية حيث يتم إرسال رسالة إلى هدف محتمل تنتحل شخصية مصدر أو منظمة حقيقية. يتم استخدام التصيد الاحتيالي لتضليل المستخدمين، كما أنه يستغل نقاط الضعف في أمان الويب اليوم. يمكن أن يتخذ تسليم رسائل التصيد الاحتيالي عدة أشكال مثل المراسلة الفورية وبروتوكول نقل الصوت عبر الإنترنت(VoIP) ، ولكن الوسيلة الأكثر شيوعاً للتصيد الاحتيالي تظل رسائل البريد الإلكتروني ومواقع التصيد الاحتيالي[20]

من خلال Conteh & Schmick (2021) على أن أساليب الهندسة الاجتماعية يمكن تقسيم هجمات الهندسة الاجتماعية إلى نوعين: هجمات الهندسة الاجتماعية القائمة على البشر وهجمات الهندسة الاجتماعية القائمة على التكنولوجيا.

الفرع الأول: الهجمات القائمة على البشر[21]

يمكن أن تكون في أشكال مختلفة منها: -

أ. انتحال الهوية Pretexting : وتُسَمَّى التذرّع حيث يستخدم المهاجمون عمليات الفحص المسبق لفهم اللغة والمنظمة والضحية، ويطلبون معلومات سرية من خلال انتحال شخصية الدعم الفني للمنظمة.

ب. الهندسة الاجتماعية العكسية (Reverse Social Engineering) :على سبيل المثال، يقومون بتخريب أنظمة المؤسسة ويعلنون أنهم هم من سيقومون بحل المشكلة.

ج. تتبع الشخص Tailgating: الدخول إلى مؤسسة ما من خلال متابعة شخص مخول بالدخول إلى موقع آمن والحصول على معلومات سرية: من خلال متابعة موظف يرتدي زياً موحداً أو شارة مطبوعة ولديه بطاقة أمنية.

الفرع الثاني: الهجمات القائمة على التكنولوجيا

إنها عملية تعتمد على التكنولوجيا ووسائل التواصل الاجتماعي والتطبيقات، وهي من أكثر الأشكال شيوعاً: -

أ. التصيّد الإحتيالي: (Phishing) هذه وسيلة للحصول على بيانات مثل كلمات المرور وتفاصيل بطاقة الائتمان. يتم ذلك من خلال ملفات موقع إلكتروني يشبه الموقع الإلكتروني لجهة موثوق بها (مثل أحد البنوك)، وهو الشكل الأكثر شيوعاً لهجمات الهندسة الاجتماعية. يتم ذلك عن طريق إرسال عدد كبير من رسائل البريد الإلكتروني ذات المظهر الحقيقي التي تحتوي على معلومات سرية أو شخصية، منتحلةً بذلك صفة مؤسسة موثوق بها. وغالباً ما يصعب التعرف عليها لأنها شائعة جداً ومتطورة، ويتم تنفيذها من خلال رسائل البريد الإلكتروني أو الروابط للتحقق من المعلومات الشخصية: اسم المستخدم وكلمة المرور.[22]

ب. طريقة الصيد بالرمح (Spear-Phishing Method) يتم ذلك من خلال محاولة الحصول على معلومات من الهدف والحصول على تفاصيل عن الضحية، ولا يستهدف دائماً المتلقي الأول فقط، بل يوفر أيضاً نقطة دخول إلى شبكة أكبر تهدف إلى إلحاق ضرر طويل الأمد بالمنظمة.

ج. إرسال الرسائل النصية القصيرة (Pretexting) يخلق هذا النوع من هجمات الهندسة الاجتماعية سيناريو يحاول فيه الهدف التعرف على المعلومات الشخصية للهدف وسرقة المعلومات الشخصية منه.

د. التصيّد الصوتي :(Vishing) يتم ذلك عبر الهاتف من خلال انتحال رقم مؤسسة معينة، مثل بنك أو شركة اتصالات، من أجل الوصول إلى معلومات المستخدم[23].

كما أن هناك أنواعاً أخرى منها الإغراء (Baiting) ؛ مشابه للتصيد الاحتيالي، ولكنه يستخدم إغراءات لاستدراج الضحايا، كذلك أسلوب المقايضة (Bartering) حيث تحتوي على معلومات مهمة مثل أدلة هواتف الشركة، والمخططات التنظيمية، وأنظمة التشغيل، وسياسات الشركة، وتقويمات الاجتماعات، ومطبوعات البيانات السرية، وأسماء تسجيل الدخول وكلمات المرور[24].

(1) N. A. G. Arachchilage and S. Love, "Security awareness of computer users: a phishing threat avoidance perspective," Comput. Human Behavior, vol. 38, pp. 304-312, Sep. 2014

(2) J. G. Mohebzada, A. E. Zarka, A. H. Bhojani, and A. Darwish, "Phishing in a university community: Two large scale phishing experiments," in Proc. Int. Conf. Innovations in Information Technology (IIT '12)، Abu Dhabi, UAE, Jun. 2012, p. 249-254

(3) Conteh, N. Y., & Schmick, P. J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), (2016).

(1) Pollock, Tommy; Levy, Yair; Li, Wei; and Kumar, Ajoy. (2020). Towards an Assessment of Judgment Errors in Social Engineering Attacks Due to Environment and Device. Type KSU Proceedings on Cybersecurity Education, Research and Practice. 3https://digitalcommons.kennesaw.edu/ccerp/2020/Research/3

(1) Salahdine, F., & Kaabouch, N. Social engineering attacks: Asurvey. Future Internet, 11(4). (2019),

(2) Conteh, N. Y., & Schmick, P. J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23). (2016)

تعد هجمات التصيد الاحتيالي هي واحدة من أنجح أساليب الهجمات القائمة على الهندسة الاجتماعية. ففي كل يوم، يتم إرسال الملايين من رسائل التصيد الاحتيالي عبر البريد الإلكتروني من قبل القراصنة، ويتم اكتشاف بعضها وحظرها بواسطة حلول تقنية مختلفة[25] .ومع ذلك، نجحت بعض رسائل التصيد الاحتيالي في التحايل على هذه الأنظمة. تبدأ هجمات التصيد الاحتيالي عادةً برسالة بريد إلكتروني تصيدية تستدرج الضحية إلى فخ. على سبيل المثال، قد تبدو رسائل التصيد الاحتيالي وكأنها واردة من مصدر حقيقي.

وتعتمد طريقة استدراج الضحية على هوية الضحية، على سبيل المثال، يطلب منه النقر على رابط لإيصال سفر أو النقر على رابط للفوز بجائزة. ويعتمد وقوع الشخص ضحية لمثل هذه الرسائل الإلكترونية الاحتيالية على خصائص السلوك البشري[26].

هـ. غوص القمامة: هجمات الغوص في القمامة هي تقنية منخفضة التقنية تُستخدم للحصول على معلومات عن الهدف[27] تتضمن العملية البحث في القمامة والبحث عن المستندات الممزقة والإيصالات وغيرها من الأوراق التي قد تحتوي على معلومات عن الهدف. قد يتخلص الأفراد من الأوراق التي قد تحتوي على معلومات حساسة مثل كلمات المرور وقسائم الدفع والفواتير وتفاصيل بطاقات الائتمان. يمكن أن تساعد هذه المعلومات القراصنة على تنفيذ هجمات الهندسة الاجتماعية ضد الأفراد بطرق متنوعة. يعد الغوص في القمامة من أكثر الطرق شيوعاً لسرقة الهوية[28].

و. برنامجScareware : يمكن تعريف Scareware على أنه نوع من هجمات الهندسة الاجتماعية التي تعتمد على المشاعر الإنسانية (مثل القلق والصدمة والتلاعب). يستخدم هذا الهجوم المشاعر الإنسانية للتلاعب بالمستخدمين لتثبيت برمجيات خبيثة. يمكن رؤية إجراء هجمات البرمجيات الخبيثة من خلال حقيقة أن القراصنة يجذبون الأهداف باستخدام تنبيهات منبثقة على مواقع الويب المختلفة. عندما ينقر الهدف على النافذة المنبثقة، يتم إعطاء معلومات مضللة للهدف. وتهدف هذه المعلومات المضللة إلى التأثير على الهدف لدفعه إلى الذعر واتخاذ إجراء ما. قد يطلب الإجراء المقصود من الهدف تقديم معلومات سرية أو شراء منتج لحل مشكلة وهمية. في هجوم التخويف، يحتاج المخترق فقط إلى إقناع الضحية بالنقر على رابط ما. ولتحقيق هذا الإقناع، يمكن للمهاجمين استخدام العديد من التقنيات لحمل الضحايا على تثبيت البرمجيات الخبيثة. تُعتبر الواجهة الرسومية لبرمجيات التخويف عنصراً أساسياً لخداع الضحايا من عدة نواحٍ. فالتمثيلات المرئية للبرمجيات (مثل النوافذ المنبثقة أو تقارير الفحص) تعطي مظهراً وكأنه تطبيق جدير بالثقة. تتبنى معظم أشكال البرمجيات الخبيثة أنظمة ألوانٍ وأنماط خطوط وشعارات تشبه العلامات التجارية المعروفة لمنتجات وبرامج مكافحة الفيروسات (مثل مايكروسوفت ونورتون لمكافحة الفيروسات)[29].

ز. ثقب الماء: هجوم ثقب الماء أو اختباء الماء هو هجوم الهندسة الاجتماعية مستوحى من طريقة صيد الحيوانات المفترسة في الغابة. في العالم الحقيقي، تنتظر الحيوانات المفترسة في الغابة بالقرب من حفرة الماء لمهاجمة فريستها، يمكن اجراء نظرة على كيفية إجراء هجوم ثقب الماء، في الخطوة الأولى، يحدد المهاجم المنظمة لاستهدافها، ثم يستخدم الدراسات الاستقصائية وغيرها من الوسائل لتحديد عادات التصفح للموظفين. استناداً إلى هذه المعلومات، يحدد المتسللون موقع الويب الذي يزوره الموظفون بشكل متكرر. في الخطوة الثانية، يعرض المهاجم موقع الويب الشرعي للخطر. قد يكون المساومة على موقع آمن شبه مستحيل، لذلك يجب على المتسللين تحديد موقع الويب الذي يمكن اختراقه (الموقع الذي يزوره الموظفون بشكل متكرر). في الخطوة الثالثة، يوجه المتسللون الموظف من موقع الويب الأصلي إلى موقع ويب ضار. يحاول هذا الموقع الخبيث تحديد نقاط الضعف في نظام الضحية. لتحديد نقاط الضعف، يستخدم المتسللون طرقاً مختلفة، أي بصمات نظام التشغيل، وتحليل سلسلة وكيل المستخدم، وما إلى ذلك. في الخطوة الرابعة، يستغل المتسلل الضعف الذي تم تحديده بواسطة الفحص السابق. بمجرد اختراق النظام، يمكن للقراصنة زيادة تقدم الهجوم عن طريق إصابة الأنظمة الأخرى على الشبكة، وتحقيق الهدف المنشود[30].

الفرع الثالث: تطبيق الهندسة الاجتماعية في مجال أمن المعلومات

يكتسب المستخدمون المعرفة الأمنية من خلال التعليم والخبرة؛ حيث يرى كومار وآخرون أنه من المهم تثقيف الموظفين حول أمن المعلومات من أجل حماية أصول المعلومات في المؤسسة. لكي تكون فعالة، يجب تدريس جميع السياسات والإجراءات والمعايير الأمنية وتعزيزها لجميع الموظفين. يجب أن يكون التعليم عملية مستمرة. لا يكفي نشر السياسات وتوقع من الموظفين قراءتها وفهمها. وبدلاً من ذلك، يحتاج الموظفون إلى أن يتعلموا سبب أهمية الأمن وكيف سيساعدهم التعليم الأمني على تجنب العواقب المكلفة على المستوى الفردي والتنظيمي. يقترح المؤلفون عدة طرق أخرى يمكن استخدامها لإبقاء الموظفين على اطلاع ووعي في جميع الأوقات[31]. وتعد الخبرة السابقة عاملاً مهماً آخر يمكن للمستخدمين من خلاله تعزيز معرفتهم الأمنية، ويقترحParrish وآخرون. [32] نموذجاً يعرض التجربة كعامل يؤثر على حكم مستخدم الإنترنت. وخلص البلادي ووير[33] إلى أن الخبرة الكبيرة في مجال أمن المعلومات تؤثر على فرص مستخدم الإنترنت في الوقوع ضحية لهجمات الهندسة الاجتماعية. يشير المؤلفون من خلال "التجارب السابقة" إلى الحوادث السابقة إن من كانوا ضحايا لشكل

(3) Pfeffel, K.; Ulsamer, P.; Müller, N. Where the user does look when reading phishing mails—An eye-tracking study. In Proceedings of the International Conference on Human-Computer Interaction (HCII), Orlando, FL, USA, 26–31 July 2019

(4) Dhillon, G.; Talib, Y.A.; Picoto, W.N. The mediating role of psychological empowerment in information security compliance intentions. J. Assoc. Inf. Syst. 2020, 21, 152–174

(1) Cross, M. Social Media Security: Leveraging Social Networking While Mitigating Risk, 1st ed.; Syngress Publishing: Rockland, MA, USA, 2014; pp. 161–191

(2) Grover, A.; Berghel, H.; Cobb, D. Advances in Computers; Academic Press: Burlington, MA, USA, 2011; Volume 83, pp. 1–50.

(1) Malin, C.H.; Gudaitis, T.; Holt, T.J.; Kilger, M. Viral Influence: Deceptive Computing Attacks through Persuasion. In Deception in the Digital Age: Exploiting and Defending Human Targets through Computer-Mediated Communications, 1st ed.; Academic Press: Burlington, MA, USA, 2017; pp. 77–124

(2) Shi, Z.R.; Schlenker, A.; Hay, B.; Bittleston, D.; Gao, S.; Peterson, E.; Trezza, J.; Fang, F. Draining the water hole: Mitigating social engineering attacks with cybertweak. In Proceedings of the Thirty-Second Innovative Applications of Artificial Intelligence Conference (IAAI-20), New York, NY, USA, 9–11 February 2020

(1) Kumar, A., Chaudhary, M. and Kumar, N. Social engineering threats and awareness: survey. European Journal of Advances in Engineering and Technology, 2, 11 (2015), 15-19.

(2) Parrish Jr, J. L, Bailey, J. L. and Courtney,J. F. A personality based model for determining susceptibility to phishing attacks. Little Rock: University of Arkansas (2009), 285-296.

(3) Albladi, S. M. and Weir, G. R. User characteristics that influence judgment of social engineering attacks cks in social networks. Human-centric Computing and Information Sciences, 8, 1 (2018).

من أشكال الهجمات الاجتماعية، مثل التصيد الاحتيالي أو سرقة الهوية. وباختصار، فإن المعرفة الأمنية هي أحد المحددات الرئيسية للسلوك الأمني، لذا فإن تطوير معرفة أمنية قوية هو مقدمة مهمة لحماية النفس من التهديدات الاجتماعية.

أ. التصعيد الاجتماعي:

تمثل هجمات الهندسة الاجتماعية مخاطر أمنية كبيرة ويجب أن تكون معالجة هذه الهجمات جزءاً من استراتيجية إدارة المخاطر للشركات والمؤسسات [34]، يجب على المؤسسات نشر ثقافة الوعي الأمني بين موظفيها. وقد تم اقتراح عدد من التقنيات لكشف هذه الهجمات ومنعها. تشمل تدابير الدفاع ضد هجمات الهندسة الاجتماعية: تشجيع التعليم والتدريب الأمني، وزيادة الوعي العام بهجمات الهندسة الاجتماعية، وتوفير الأدوات اللازمة لاكتشاف هذه الهجمات وتجنبها، وكيفية الحفاظ على أمن المعلومات الحساسة، التعلم والإبلاغ عن الأنشطة المشبوهة. بالإضافة إلى الحد من مخاطر الهجمات العدائية ضد جميع الموظفين من خلال رسائل البريد الإلكتروني التوعوية وإعادة توجيه رسائل البريد الإلكتروني الاحتيالية المعروفة[35].

وللكشف عن الهجمات الهاتفية، من الضروري التحقق من هوية المتصل باستخدام قوائم جهات الاتصال المسجلة للتعرف على المتصل، أو التعرف على المكالمات غير المتوقعة أو غير المرغوب فيها، أو طلب معاودة الاتصال أو طرح أسئلة ذات إجابات خاصة. الطريقة الأكثر فعالية لإحباط مثل هذه الهجمات هي تجنب الرد على هذه المكالمات. في حالة هجمات مكاتب المساعدة، يمكن منع المكالمات الخبيثة من خلال تخصيص أرقام تعريف شخصية للمتصلين المعروفين. [36].مطلوب من مكتب المساعدة حماية النطاق أثناء إجراء طلبات الاتصال. في الهجمات القائمة على البريد الإلكتروني، تستخدم بعض الشركات عناوين البريد الإلكتروني المصيدة، والمعروفة أيضاً باسم مصائد البريد العشوائي، لجمع وتوزيع البريد العشوائي على الموظفين.

ب. مصائد البريد المزعج

عندما يتم إرسال بريد إلكتروني من إحدى القوائم، يعتبره الخادم خبيثاً ويقوم بحظره مؤقتاً. تشمل العلاجات الأخرى: التحقق من مصدر رسائل البريد الإلكتروني قبل النقر على الروابط أو فتح المرفقات؛ والتحقق من رؤوس البريد الإلكتروني؛ والاتصال بالمرسلين المعروفين في حالة الشك؛ وتجاهل رسائل البريد الإلكتروني التي تحتوي على إعلانات مبهرجة أو حائزة على جوائز. في مواجهة هجمات التصيّد الاحتيالي، تم اقتراح أدوات مكافحة التصيّد الاحتيالي لوضع قائمة سوداء لمواقع التصيّد الاحتيالي وحظرها. ومن أمثلة هذه الأدوات مرشح McAfee لمكافحة التصيد الاحتيالي، ومرشح التصيد الاحتيالي من Microsoft، و[37] Web Sens، ولقد اقترح المؤلفون تعليم الطلاب كيفية تنفيذ هجوم التصيّد بالحربة من خلال التعلم بالممارسة. لقد طوروا إطاراً يتعلم فيه الطلاب كيفية التصيّد الاحتيالي.

تعمل رسائل البريد الإلكتروني من خلال تنفيذ هجمات على شركة افتراضية. بعد جمع كل المعلومات الممكنة من موقع الشركة، أطلق الطلاب رسائل بريد إلكتروني تصيدية لمحاكاة الموظفين وبعد ذلك فحص جميع رسائل البريد الإلكتروني المستلمة لتحديد طبيعتها[38]، اقترح المؤلفون [39]تقنية اكتشاف تعتمد على خوارزميات التعلم الآلي. وتعتمد هذه التقنية على التعلّم غير الخاضع للإشراف وليس لديها معرفة مسبقة بالهجمات المرصودة. وقارن المؤلفان أداء ست خوارزميات للتعلم الآلي للكشف عن هجمات التصيد الاحتيالي من حيث السرعة والموثوقية والدقة: آلة ناقل الدعم، وآلة ناقل الدعم المتحيزة، والشبكات العصبية الاصطناعية، والتدرج المترافق المقيس، وخريطة التنظيم الذاتي. لقد أظهروا أن خوارزمية آلة ناقل الدعم تحقق نتائج أفضل مقارنة بالخوارزميات الأخرى[40]، اقترح المؤلفون طريقة للكشف عن هجمات التصيد الاحتيالي لبيانات الاعتماد في جلسات المؤسسة. تعمل طريقة الكشف المقترحة، والتي تسمى اكتشاف الشذوذ (DAS)، عن طريق تحليل الخصائص المحتملة لهجمات التصيد الاحتيالي من أجل استخلاص عدد من المعلومات والميزات التي يستخدمها المهاجم. إنها طريقة لتسجيل الشذوذ غير المعلمي فهي تستخدم لتصنيف التنبيهات، وبالنسبة للهجمات اللاحقة، قد يتم منعها من خلال تدريب الموظفين على عدم السماح مطلقاً بالوصول إلى شخص بدون شارة دون استثناءات وطلب أقفال ومعرفات لجميع الموظفين[41]. بالنسبة لهجمات تصفح الكشف، يُطلب من الأفراد أن يكونوا أكثر وعياً بما يحيط بهم، بما في ذلك الأشخاص أو الكاميرات عند إدخال معلومات حساسة. بالنسبة لهجمات الغوص في القمامة، يجب تدمير المستندات والمواد الحساسة المهملة بالكامل باستخدام آلات تمزيق الورق، ويجب تأمين أجهزة الذاكرة أو محوها، ويجب قفل الملفات المهمة بشكل آمن وعدم تركها سهلة الوصول، فقد يتم منع الهجمات المستندة إلى أحصنة طروادة عن طريق رفض السماح لشخص ما باستخدام أجهزة الكمبيوتر الشخصية أو أجهزة الكمبيوتر الخاصة بالعمل، واستخدام برنامج مكافحة الفيروسات لفحص USB قبل فتحه واتباع تعليمات وتحذيرات مكافحة الفيروسات، وفحص أي حزم بريدية غير متوقعة، وعدم التقاط واستخدام العثور عليها الوسائط الرقمية. لمنع هجمات البرامج المزيفة، يحتاج الأفراد إلى فحص الشاشة بعناية والتحقق مما إذا كانت نافذة البرنامج شرعية لأن مواقع الويب الحقيقية تحتوي دائماً على شيء مميز عن المواقع المزيفة. مكافحة الفيروسات قد تكون محدودة بسبب جهل الإنسان؛ وقد يكتشفون هذه الهجمات ويرسلون تحذيرات، وهو ما يتجاهله معظم المستخدمين عن طريق إغلاق النافذة والمضي قدماً. يمكن أخذ إجراءات الوقاية الأخرى بعين الاعتبار، بما في ذلك

(4) Osuagwu, E.; Chukwudebe, G.; Salihu, T.; Chukwudebe, V. Mitigating social engineering for improved cybersecurity. In Proceedings of the IEEE Conference on Cyberspace, Abuja, Nigeria, 4-7 November 2015; p. 91-100.
(1) Foozy, C.FM, Ahmad, R.; Abdollah, M.F: Yusof, R.; Mas'ud, M.Z. Generic taxonomy of social engineering attack and defence mechanism for handheld computer study. In Proceedings of the Malaysian Technical Universities International Conference on Engineering and Technology, Batu Pahat, Malaysia, 13-15 November 2011; p. 1-6.
(2) Kaushalya, S.A.; Randeniya, R.M.; Liyanage, A.D. An Overview of Social Engineering in the Context of Information Security. In Proceedings of the 5th IEEE International Conference on Engineering Technologies and Applied Sciences, Bangkok, Thailand, 22-23 November 2018; p. 1-6.
(1) Lohani, S. Social Engineering: Hacking into Humans. Int. J. Adv. Stud. Sci. Res. 2019, 5.
(2) Chothia, T.; Stefan-loan, P.; Oultram, M. Phishing Attacks: Learning by Doing. In Proceedings of the USENIX Workshop on Advances in Security Education, Baltimore, MD, USA, 13 August 2018; p. 1-2.
(3) Smutz, C.; Stavrou, A. Malicious PDF detection using metadata and structural features. In Proceedings of the 28th ACM annual computer security applications conference, Orlando, FL, USA, 3-7 December 2012; p. 239-248
(4) Sharma, Ho, G.; Javed, A.; Paxson, M.; Wagner, V.; D. Detecting credential spearphishing in enterprise settings. In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 15-17 August 2017; p. 469-485.
(5) Ivaturi, K.; Janczewski, L. A taxonomy for social engineering attacks. In Proceedings of the International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, Ontario, Canada, 18-20 June 2011; p. 1-12

التحقق مما إذا كان موقع الويب يحتوي على شعارhttps ، وعدم النقر قبل فحص عنوانURL ، وتحديث نظام تشغيل الكمبيوتر وبرامج الأمان بانتظام وتشجيع بعض المنظمات الأمنية الشركات على تبني استراتيجية الدفاع المتعمق لمراقبة شبكتها وإعداد نفسها لهجمات محتملة مع إهمال الجانب الإنساني [42]. اقترح المؤلفون تحديد متطلبات إطار عمل لمكافحة هجمات الهندسة الاجتماعية يمكنه تحليل مخاطر الهجمات والتخفيف من حدتها. وطوروا تقنية دفاعية جديدة متعددة الطبقات تسمى تقييم المخاطر المرتكز على الهندسة الاجتماعية. (SERA) تبدأ SERA في الخطوة التالية، يتم تحديد الأصول الهامة لتقييم معلومات الشركة. ثم يتم وضع كل أصل في حاوية ويتم تحديد ناقل هجوم الهندسة الاجتماعية المقابل. يتم تحديد الهجمات المحتملة من قبل خبراء الأمن المحليين ويتم الحصول على تحليل للمخاطر.

واقترح المؤلفون نهج القائمة البيضاء للتدفق لتعزيز أمان الشبكة داخل الشركات. يهدف أسلوب القائمة البيضاء للتدفق إلى تحديد حركة المرور المشروعة من حركة المرور الضارة القادمة إلى شبكة الشركة، يتم استخدام أربع خصائص لتحديد هذه القوائم البيضاء: عنوان العميل وعنوان الخادم ورقم منفذ الخادم والبروتوكول المستخدم لإعادة توجيه حركة المرور. يتم تنفيذ النهج المقترح من خلال التقاط حركة مرور الشبكة لفترة زمنية محددة مسبقاً وتجميع حركة المرور هذه في تدفقات إذا تم تحديد حركة المرور هذه على أنها شرعية. ويستند ذلك إلى تعلم كيفية التمييز بين حركة المرور المشروعة وحركة المرور الخبيثة وحركة المرور الخبيثة المرصودة. [43] وإنذارات عصبية في حالة وجود Tab Shots للتمييز بين الصفحات الشرعية والصفحات الضارة. يعد Tab Shots امتداداً مثبتاً في المتصفح يقارن مظهر صفحات الويب ويسلط الضوء على أي تغييرات ملحوظة لإثارة انتباه المستخدم قبل المتابعة. ولقد ناقش مشكلة إضفاء الطابع الرسمي على الإجراءات الناتجة عن هجمات الهندسة الاجتماعية. واقترحوا نمذجة هذه الإجراءات من خلال الاحتمالات والنماذج الرسومية مثل النماذج البايزية. وقاموا بتحليل الملف الشخصي للمستخدم لتقدير نقاط الضعف والميزات النفسية. يتم تقدير حماية ملف تعريف المستخدم ضد الهجوم من خلال أربعة عناصر: السمات النفسية(F) ، ونقاط الضعف الحرجة(V) ، وإجراءات الهجوم(A) ، ومسؤولية المستخدم عند الهجمات الناجحة[44] . وأيضاً تم تطوير برنامج توعوي بالهندسة الاجتماعية (SEAP) للمدارس بهدف زيادة وعي الطلاب من خلال توفير المعلومات الحيوية التعليم والتدريب في مرحلة مبكرة [45].

ج. التحديات والقضايا الأخلاقية:

تُستخدم التفاعلات الاجتماعية التي تعد وسيلة للإيماءات الودية كإعدادات لانتزاع معلومات حيوية وحساسة من الضحية المخدوعة. إن أسلوب استخدام الأشخاص للحصول على معلوماتهم الخاصة والسرية التي تدعي أنها مصادر موثوقة هو السياق الرئيسي للهندسة الاجتماعية الضحية؛ يتم إجبار فرد أو منظمة على الكشف عن تفاصيل شخصية عن طريق الإقناع أو التفاعل الاجتماعي أو الطلبات التي تتضمن طرفاً ذا صلة بتكنولوجيا المعلومات. أن السبب الرئيسي وراء هذه الهجمات هو عدم وعي الضحية. مما يجعل الناس أنفسهم عرضة لهذه الهجمات من خلال عدم التعامل مع الموضوع على محمل الجد. ومن ثم فإن الكثير ممن لم يتوقعوا أبداً أن يكونوا ضحية لمثل هذا الموقف ينتهي بهم الأمر إلى أن يصبحوا ضحية ويظلون غير مدركين له. ونتيجة لذلك، فإن غالبية الجمهور واجهوا وما زالوا يواجهون عواقب شخصية واقتصادية واجتماعية كفرد أو منظمة. قد تكون الضحية دائما تحت الانطباع بتمرير معلومات لا قيمة لها لشخص آخر أو ليس لديه أي فكرة عن إمكانية استخدامها في أنشطة غير لائقة أو غير قانونية، وبالتالي يكون على استعداد للكشف عنها. يكرس المهاجم استكشاف التقنيات المختلفة ويجمع المعلومات من العديد من المصادر ويجمعها معًا مما يؤدي إلى خرق أمني كارثي للغاية [46]. ومن الأمثلة الجيدة على ذلك هجوم برنامج الفدية على "مركز هوليوود المشيخي الطبي" في عام 2016، حيث تم احتجاز نظام الكمبيوتر الخاص به كرهينة من قبل المتسللين. ومن الأمثلة الحديثة الأخرى هجوم برنامج الفدية " Do Not Cry" الذي يستهدف الهواتف المحمولة. لو أن الفرد قد استشعر النشاط الخبيث من خلال عدم العيش تحت ذريعة عدم وجود احتمالات لمثل هذه الأحداث، واستشعاره على الفور لكان قادراً على منع مثل هذه النتائج الكارثية. إلا أن المهندس الاجتماعي؛ فالمهاجم هو مناور بشري ماهر، يتغذى على نقاط الضعف البشرية مستخدماً العديد من الشرارات النفسية لتعمي الحكم البشري[47]. أثبتت العديد من الأبحاث أن جوانب مثل السمات الشخصية والتركيبة السكانية والعادات عبر الإنترنت لكل فرد أو منظمة تتم مراقبتها في استهداف الهجمات الناجحة [48]

د. الخصوصية والتلاعب النفسي:

لبدء هجوم الهندسة الاجتماعية، يحتاج المهاجم إلى شكل من أشكال التأثير على الهدف. يناقش هذا القسم الطرق المختلفة للتلاعب النفسي على الضحية وعرضها للخطر. الجوانب السلوكية البشرية البارزة المستخدمة لبدء هجوم الهندسة الاجتماعية هي التأثير الاجتماعي والإقناع والموقف والسلوك والثقة والاحتيال وصنع القرار والعواطف واللغة والاستدلال وما إلى ذلك[49]. تستخدم الجوانب السلوكية المذكورة أيضا في الهجمات الإلكترونية القائمة على الهندسة الاجتماعية . استناداً إلى سمات الضحية، يستغل المهاجمون الضعف البشري الأنسب. يمكن للمهاجمين أيضا استخدام نقاط ضعف متعددة في مراحل مختلفة من الهجوم.

تعتمد الهندسة الاجتماعية على طرق الإقناع للتلاعب بالضحايا لأداء أعمال أو الكشف عن معلومات سرية. الإقناع هو طريقة معروفة تستخدم في العديد من المجالات الأخرى، مثل المبيعات والتسويق والتأمين وما إلى ذلك[50]. ومن أمثلة عمليات التلاعب النفسي، حيث وقعت شركة تويوتا بوشوكو، وهي

(1) Abeywardana, K., Tunnicliffe, M. A layered defense mechanism for a social engineering aware perimeter.In Proceedings of the SAI Computing Conference, London, UK, 13-15 July 2016; p. 1054-1062.
(1) Barbosa, R.R.R; Sadre, R.; Pras, A. Flow whitelisting in SCADA networks. Int. J. Crit. Infrastruct. Prot. 2013, 6, 150-158.
(2) Abramov, M.; Azarov, A. Social engineering attack modeling with the use of Bayesian networks. In Proceedings of the IEEE International Conference on Soft Computing and Measurements, Petersburg, Russia, 25-27 May 2016; p. 58-60
(3) Algarni, A., Xu, Y.; Chan, T. Measuring source credibility of social engineering attackers on Facebook. In Proceedings of the IEEE Hawaii International Conference on System Sciences, Koloa, HI, USA, 5-8 January 2016; p. 3686-3695
(1) Frumento, E. "Dogana Project," 16 February 2016. [Online]. Available: https://www.dogana-project.eu/index.php/social-engineering-blog/11-social- engineering/9-which-could-be-the-consequences-of-a- social-engineering-attack.
(2) Hadnagy C., Unmasking the Social Engineer: The Human Element of Security, John Wiley & Sons Inc., 2014.
(3) Green J., "Online Owls," 25 May 2017. [Online]. Available: https://www.onlineowls.com/5-reasons- cybersecurity/.
(4) Wang, Z.; Zhu, H.; Sun, L. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access2021, 9, 11895–11910
(1) Ferreira, A.; Coventry, L.; Lenzini, G. Principles of persuasion in social engineering and their use in phishing. In Proceedings of the Name of the Human Aspects of Information Security, Privacy, and Trust (HAS), Los Angeles, CA, USA, 2–7 August 2015.

مورد رئيسي للمكونات لشركة تويوتا، ضحية لخطة BEC (تسوية البريد الإلكتروني التجاري)، في هذا الاعتداء على البريد الإلكتروني للتصيد الاحتيالي، نجح الجناة في خداع الشركة من بين أكثر من 37 مليون. في 14 أغسطس 2019، خدع هؤلاء المحتالون فرداً في تويوتا بتفويض مالي لتغيير تفاصيل الحساب لتحويل الأموال إلكترونياً. يكشف تقرير صادر عن مكتب التحقيقات الفيدرالي أن عمليات الاحتيال في BEC قد ألحقت خسارة مذهلة تبلغ حوالي 5.3 مليار دولار بالاقتصاد العالمي في السنوات الست الماضية. تشير الدراسات الاستقصائية إلى أن حوالي 75٪ من الشركات تواجه محاولة هجومBEC واحدة على الأقل سنوياً[51] .

الفرع الرابع: التعاون بين الهندسة الاجتماعية والتقنيات الأمنية [52]

أ. إنشاء مركز وطني لحماية البنية التحتية للمعلومات الحرجة وفقاً للمادة 70/ أ من قانون تقنية المعلومات.
ب. التنبيهات والتهديدات السيبرانية وإشعارات التدابير المضادة الصادرة عن CERT-In.
ج. إصدار توجيهات بشأن الواجبات والمسؤوليات الأساسية لكبير مسؤولي أمن المعلومات (CISOs)في مجال حماية التطبيقات/البنية التحتية والامتثال.
د. إجراء عمليات تدقيق منتظمة قبل وبعد التدقيق في المواقع الإلكترونية والتطبيقات الحكومية.
ه. منظمة تدقيق أمني تدعم وتدقق في تنفيذ أفضل الممارسات في مجال أمن المعلومات.
و. تصميم خطة إدارة الأزمات للاعتداءات السيبرانية.
ز. إجراء تدريبات منتظمة للأمن السيبراني ومحاكاة لاختبار الموقف الأمني للمؤسسات الحكومية ومؤسسات القطاع الحيوي واستعداداتها.
ح. إجراء برامج تدريبية متكررة حول أمن البنية التحتية للمعلومات والتهديدات السيبرانية لمسؤولي الشبكات/النظم، والوكالات الحكومية ورؤساء الإدارات الرئيسية.

خاتمة

ويصف هذا البحث الإطار المفاهيمي للهندسة الاجتماعية والأساليب والأدوات المستخدمة في هجمات الهندسة الاجتماعية التي تستهدف أنظمة التوثيق، إلى جانب دراسات بحثية حول هجمات التصيد الاحتيالي التي تواجهها شركات تكنولوجيا المعلومات العالمية البارزة. علاوةً على ذلك، سيتم وصف تحديد تقنيات الدفاع ضد هذه الهجمات، إلى جانب منهجيات الكشف عنها. لا يمكن تحييد هجمات الهندسة الاجتماعية، سواء كانت مباشرة أو من خلال وسطاء مثل الهواتف أو أجهزة الكمبيوتر المتصلة بالإنترنت، بشكل كامل من خلال تدابير تكنولوجيا المعلومات المتخصصة والأمن المادي وحدها. يجب أن يكون التركيز الرئيسي على التعليم والتدريب والمعرفة المستمرة لكل من الموظفين والجمهور العام داخل المؤسسة. يمكن أن يساعد استمرار الوعي العام بالمخاطر في مجال الإنترنت والاتصالات السلكية واللاسلكية واستراتيجيات مواجهتها ودعم أدوات الكشف المتخصصة لهجمات الهندسة الاجتماعية المختلفة في منع فقدان البيانات.

التوصيات

تشكل الهندسة الاجتماعية تهديداً كبيراً لأمن المعلومات في الشركات والمؤسسات والأفراد. فمع تحسن الأمن التكنولوجي، سيختار المزيد والمزيد من الأشخاص الخبيثين أسهل طريقة لاستخدام الأشخاص للحصول على المعلومات أو الوصول إلى الموارد لتحقيق ما يريدون. ولمنع مثل هذه الفرص، يجب السيطرة على الهندسة الاجتماعية أو على الأقل الحد منها. عندما يتعلق الأمر بأمن المعلومات، إذ يركز الكثير من الناس على الأمن التقني حيث أن الحلول التقنية مثل جدران الحماية وقواعد المصادقة والتشفير وقيود الوصول والأذونات ضرورية لأمن المعلومات في المؤسسة لأنها يمكن أن تمنع الهجمات.

ولضمان تغطية الحماية التقنية، هناك حاجة إلى الأمن الإداري، مثل المراقبة والضوابط والرصد والسياسات والإجراءات.

المراجع العربية:

1. الكندي، سالم بن سعيد بن علي، وحليمة سليمان البلوشي. "الوعي بثقافة الهندسة الاجتماعية لدى طلبة كليات التعليم التقني بسلطنة عمان: دراسة حالة لطلبة الكلية التقنية بالمصنعة." مجلة الآداب والعلوم الاجتماعية مج11, ع2 (2020).
2. المركز الوطني الإرشادي للأمن السيبراني (2020)، الهندسة الاجتماعية توعوي ملصق https://cert.gov.sa/ar/awareness/social_engineering/
تم الاطلاع عليه في 22/8/2024 ال ساعه5:43

المراجع الأجنبية:

1. N. A. G. Arachchilage and S. Love, "Security awareness of computer users: a phishing threat avoidance perspective," Comput. Human Behavior, vol. 38, p. 304-312, Sep. 2014.
2. Frumento, E. "Dogana Project," 16 February 2016. [Online]. Available: https://www.dogana-project.eu/index.php/social-engineering-blog/11-social- engineering/9-which-could-be-the-consequences-of-a- social-engineering-attack.
3. Wang, Z. Sun, L. and Zhu, H. "Defining social engineering in cyber- security," IEEE Access, vol. 8, p. 85094-85115, (2020)
4. Abeywardana, K., Tunnicliffe, M. A layered defense mechanism for a social engineering aware perimeter.In Proceedings of the SAI Computing Conference, London, UK,; pp. 1054-1062. 13-15 July 2016
5. Abramov, M.; Azarov, A. Social engineering attack modeling with the use of Bayesian networks. In Proceedings of the IEEE International Conference on Soft Computing and Measurements, Petersburg, Russia; pp. 58-60, 25-27 May 2016
6. Albladi, S. M. and Weir, G. R. User characteristics that influence judgment of social engineering attacks cks in social networks. Human-centric Computing and Information Sciences, 8, 1, 5. (2018)
7. Algarni, A., Xu, Y.; Chan, T. Measuring source credibility of social engineering attackers on Facebook. In Proceedings of the IEEE Hawaii International Conference on System Sciences, Koloa, HI, USA; pp. 3686-3695, 5-8 January 2016

(2) FBI. Business Email Compromise and Real Estate Wire Fraud. (2022).
(3) KING, D. The American State and Social Engineering: Policy Instruments in Affirmative Action. Governance, 20(1), 109-126(2007).

8. Atkins, B. & Huang, W. A study of social engineering in online frauds. Open Journal of Social Sciences, 1(3), 23-32. (2013).
9. Barbosa, R.R.R; Sadre, R.; Pras, A. Flow whitelisting in SCADA networks. Int. J. Crit. Infrastruct. Prot. 2013, 6, 150-158.
10. Bhise, K., "A Method for Recognize Malignant Facebook Application," p. 41-44, 2016
11. Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. Journal of Investigative Psychology and Offender Profiling, 15(1), 20-45. (2017).
12. Centre, C. S. and Jones, A., "Information Security and Digital Forensics in the world of Cyber Physical Systems," p. 10-14, 2016.
13. Chothia, T.; Stefan-loan, P.; Oultram, M. Phishing Attacks: Learning by Doing. In Proceedings of the USENIX Workshop on Advances in Security Education, Baltimore, MD, USA, 13 August; pp. 1-2. 2018
14. Christopher,h., Social Engineering: The Art of Human Hacking, WILEY Publishing, (2017),
15. Cialdini, R. B. Influence. New York, NY: HarperCollins. (2009).
16. Conteh, N. Y., & Schmick, P. J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), (2016).
17. Conteh, N. Y., & Schmick, P. J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), (2016).
18. Cross, M. Social Media Security: Leveraging Social Networking While Mitigating Risk, 1st ed.; Syngress Publishing: Rockland, MA, USA, 2014; p. 161–191
19. Dhillon, G.; Talib, Y.A.; Picoto, W.N. The mediating role of psychological empowerment in information security compliance intentions. J. Assoc. Inf. Syst., 21, 152–174, (2020).
20. FBI. Business Email Compromise and Real Estate Wire Fraud. (2022).
21. Ferreira, A.; Coventry, L.; Lenzini, G. Principles of persuasion in social engineering and their use in phishing. In Proceedings of the Name of the Human Aspects of Information Security, Privacy, and Trust (HAS), Los Angeles, CA, USA, 2–7 August 2015.
22. Foozy, C.FM, Ahmad, R.; Abdollah, M.F: Yusof, R.; Mas'ud, M.Z. Generic taxonomy of social engineering attack and defence mechanism for handheld computer study. In Proceedings of the Malaysian Technical Universities International Conference on Engineering and Technology, Batu Pahat, Malaysia, 13-15 November; p. 1-6.2011.
23. Frumento, E. Estimates of the Number of Social Engineering Based Cyber-Attacks into Private or Government Organizations. Dogana Project. (2018)
24. Ghafir, I. Prenosil, V, Alhejailan, A. and Hammoudeh, M. "Social Engineering Attack Strategies and Defence Approaches," 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, p. 145-149, 2016.
25. Grande,C. E. L., and Guadrón, R. S., "Social Engineering: The Silent Attack," no. Concapan Xxxv, 2015.
26. Green J., "Online Owls," 25 May 2017. [Online]. Available: https://www.onlineowls.com/5-reasons- cybersecurity/.
27. Grover, A.; Berghel, H.; Cobb, D. Advances in Computers; Academic Press: Burlington, MA, USA; Volume 83, pp. 1–50. (2011).
28. Hacking the human operating system: The role of social engineering within cybersecurity", Technical report, Intel Security, 2015.
29. Hadnagy C., Unmasking the Social Engineer: The Human Element of Security, John Wiley & Sons Inc., 2014.
30. Hutchings, A., Hacking and fraud: Qualitative analysis of online offending and victimization. In K. Jaishankar & N. Ronel (eds.) Global criminology: Crime and victimization in a globalized era (pp. 93-114). (2013)
31. Hutchings, A., Hacking and fraud: Qualitative analysis of online offending and victimization. In K. Jaishankar & N. Ronel (eds.) Global criminology: Crime and victimization in a globalized era (pp. 93-114). (2013)
32. Ivaturi, K.; Janczewski, L. A taxonomy for social engineering attacks. In Proceedings of the International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, Ontario, Canada, 18-20 June; p. 1-12,2011
33. J. G. Mohebzada, A. E. Zarka, A. H. Bhojani, and A. Darwish, "Phishing in a university community: Two large scale phishing experiments," in Proc. Int. Conf. Innovations in Information Technology (IIT '12), Abu Dhabi, UAE, Jun. 2012, pp. 249-254
34. Kaushalya, S.A.; Randeniya, R.M.; Liyanage, A.D. An Overview of Social Engineering in the Context of Information Security. In Proceedings of the 5th IEEE International Conference on Engineering Technologies and Applied Sciences, Bangkok, Thailand, 22-23 November; pp. 1-6. 2018
35. KING, D. The American State and Social Engineering: Policy Instruments in Affirmative Action. Governance, 20(1), 109-126(2007).
36. KING, D. The American State and Social Engineering: Policy Instruments in Affirmative Action. Governance, 20(1), 109-126(2007).
37. Kumar, A., Chaudhary, M. and Kumar, N. Social engineering threats and awareness: survey. European Journal of Advances in Engineering and Technology, 2, 11, 15-19. (2015)

38. Leukfeldt, E. R. ,Cybercrime and social ties: Phishing in Amsterdam. Trends in Organized Crime, 17(4), 231-249. (2014a).
39. Lohani, S. Social Engineering: Hacking into Humans. Int. J. Adv. Stud. Sci. Res. 2019, 5.
40. Lusthaus, J. Industry of anonymity: Inside the business of cybercrime. Cambridge, MA: Harvard University Press. (2018).
41. Malin, C.H.; Gudaitis, T.; Holt, T.J.; Kilger, M. Viral Influence: Deceptive Computing Attacks through Persuasion. In Deception in the Digital Age: Exploiting and Defending Human Targets through Computer-Mediated Communications, 1st ed.; Academic Press: Burlington, MA, USA; pp. 77–124, (2017)
42. Maseno, E. M. "Vishing attack detection model for mobile users," M.S. thesis, Comput. Inf. Manage., KCA Univ., Nairobi, Kenya, Nov. 2017. [Online]. Available:http://41.89.49.13:8080/xmlui/handle/123456789/1276
43. McCrae R. R. and John, O. P. "An introduction to the five-factor model and its applications," J. Personality, vol. 60, no. 2, p. 175-215, Jun. 1992.
44. Nabie Y Conteh, Paul J Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks", International Journal of Advanced Computer Research, Vol.6 pp.23-31, 2016.
45. Osuagwu, E.; Chukwudebe, G.; Salihu, T.; Chukwudebe, V. Mitigating social engineering for improved cybersecurity. In Proceedings of the IEEE Conference on Cyberspace, Abuja, Nigeria, 4-7 November; pp. 91-100. 2015
46. Parrish Jr, J. L, Bailey, J. L. and Courtney,J. F. A [personality based model for determining susceptibility to phishing attacks. Little Rock: University of Arkansas, 285-296. (2009)
47. Pfeffel, K.; Ulsamer, P.; Müller, N. Where the user does look when reading phishing mails—An eye-tracking study. In Proceedings of the International Conference on Human-Computer Interaction (HCII), Orlando, FL, USA, 26–31 July 2019
48. Pollock, Tommy; Levy, Yair; Li, Wei; and Kumar, Ajoy. (2020). Towards an Assessment of Judgment Errors in Social Engineering Attacks Due to Environment and Device. Type KSU Proceedings on Cybersecurity Education,ResearchandPractice.https://digitalcommons.kennesaw.edu/ccerp/2020/Research/3.
49. Prashant, K, D., "Prashant's algorithm for password management system", International Journal of Engineering Science, pp.2424, 2016.
50. Rachsuda, J. "User preferences profiling based on user behaviors on facebook page categories," pp. 248-253, 2017.
51. Salahdine, F., & Kaabouch, N. Social engineering attacks: Asurvey. Future Internet, 11(4). (2019),
52. Sarathchandra, D. Haltinner, K. and Lichtenberg, N. "College students' cybersecurity risk perceptions, awareness, and practices," in Proc. Cybersecurity 3rd Symp. (CYBERSEC '16), Coeur d'Alene, ID, 2016, p. 68-73.
53. Sharma, Ho, G.; Javed, A.; Paxson, M.; Wagner, V.; D. Detecting credential spearphishing in enterprise settings. In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 15-17 August; pp. 469-485. 2017
54. Shi, Z.R.; Schlenker, A.; Hay, B.; Bittleston, D.; Gao, S.; Peterson, E.; Trezza, J.; Fang, F. Draining the water hole: Mitigating social engineering attacks with cybertweak. In Proceedings of the Thirty-Second Innovative Applications of Artificial Intelligence Conference (IAAI-20), New York, NY, USA, 9–11 February, 2020
55. Smutz, C.; Stavrou, A. Malicious PDF detection using metadata and structural features. In Proceedings of the 28th ACM annual computer security applications conference, Orlando, FL, USA, 3-7 December; pp. 239-248.2012
56. Stewart J. and Dawson M., "How the modification of personality traits leave one vulnerable to manipulation in social engineering," Int. J. Inf. Privacy, Secur. Integrity, vol. 3, no. 3, p. 187-208, Jan. 2018.
57. Tsinganos, N. Sakellariou, G. Fouliras, P. and Mavridis, I. "Towards an automated recognition system for chat-based social engineering attacks in enterprise environments," in Proc. 13th Int. Conf. Availability, Rel. Secur.,. New York, NY, USA, Aug. 2018, p. 53
58. Wang, Z.; Zhu, H.; Sun, L. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access2021, 9, 11895–11910

Whitty, M. T., The scammers persuasive techniques model. British Journal of Criminology, 53, 665-684. (2013).